Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Digital Signature - A Tool of Authenticity in the Virtual world

Saundarya Awasthi[a]

[a]Bharati Vidyapeeth University, Pune, India

Received 17 June 2022; *Accepted* 29 June 2022; *Published* 11 July 2022

With the world going digital every person exchange information instantly due to which there is an increase in its vulnerability, which is where the importance of validity of digital signature comes into place. A digital signature is a document like contracts and receipts that, uses mathematical terms to interpret and verify that an email message is really from the person who supposedly sent it and that hasn't been changed. The Government and military organisations have spent a lot of resources to make such algorithms effective through encryption and decryption. Services like authentic key agreement, entity authentication, and authentic key delivery used under cryptographic protocols are a few techniques in Digital Signature.[1] This technique performs its way to integrity by using public and private keys to cypher the validity of a transaction. The following article highlights the scope, meaning, nature, and significance of the electronic environment. Also, it attempts to grab its effect and impact in cyberspace and the limitations in the Indian legal system.

Keywords: *digital signature, cryptographic, public key, private key.*

[1] Dr. Abhishek Roy & Sunil Karforma, 'A survey on digital signatures and its applications' (*Research Gate*, January 2012) <https://www.researchgate.net/publication/233391380_A_survey_on_digital_signatures_and_its_applications> accessed 03 June 2022

INTRODUCTION

In the traditional times, seals, stamps, or physical signatures were a few tools that were used to create the authenticity of a legal paper or document of contract, for us it is the digital signature as a tool of validity in the virtual world. A signature defines as a representation of the identity of a person to the document which owes legal responsibility discharging out of it. Today's world demands a flexible and responsive solution where the role of the Digital Signature comes into place. It establishes a link between the subscribers of digital signs that want to be authenticated by affixing a sign. For eg.- A, a company has its business partners based abroad and whenever they need to counter sign a document it will end up taking weeks to get the paperwork done physically which will be waste of time, but if the companies used Digital signature it will be a deal in a matter of minutes, the transaction is completely paperless.[2] Thus in order to achieve such authentication and security of e-transactions, this mechanism was introduced by the Information Technology Act of 2000. A digital signature just like a handwritten signature binds a person or entity to electronic data. The digital signature is a combination of public key and public key via a hashing process that produces a series of encryption on one side and decryption on the other side to verify a report.[3] A public key is like an email and a private key is like a password to that email id. Digital signature has its focuses on the technological aspect which helps achieve the reputation, validity, and verification of electronic records. It is basically a software distribution that includes different contact details and in order to verify the process of encryption and decryption are constituted which results in the validity of a document. In the end, that signature is certified by the Certifying Authority of the Government.

[2] Vijaykumar Shrikrushna Chowbe, 'Digital Signature :Nature &Scope Under the IT Act, 2000' (*SSRN E-Journal,* 23 September 2010) <.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1680825> accessed 01 June 2022

[3] J. Chandrashekhara, & et.al., 'A Comprehensive Study on Digital signature' (2021) 9 (1) International Journal of Innovative Research in Computer Science & Technology, <https://www.ijircst.org/DOC/7-a-comprehensive-study-on-digital-signature.pdf > accessed 01 June 2022

HISTORICAL BACKGROUND

The existence of such a concept began in 1976 when Whitefield Diffie and Martin Hellman published a paper called New Ways in Cryptography which included a new method of distributing cryptographic keys. The article thereby lead to the development of an effective asymmetric algorithm and gave a reason for digital signature schemes. Later on, in 1977 Ronal Rivest, Adi Shamir, and Len Adleman came up with the RSA concept of algorithm. The method was in progress of becoming more safe and efficient and for this, the hash function was applied to the RSA algorithm method to the original message and was proved to be safe. ShafiGoldwasser, Silvio Micali, and Ronald Rivest were the first to define an early development in digital signature in 1984. Lotus 1.0cwas the first well-known software that was enabled.[4]

THE PROCESS OF CREATION

The term has been defined by S. 2 (1) (p)[5] of the Information Technology Act of 2000 as follows:

Section 2(1)(p) a "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3[6].

A digital signature in fact consists of two keys named public key and private key which are the essentials of such a verification process. A private key is shared privately who is the subscriber and from it, the public key will be generated publicly. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

[4] Deeksha Singh, 'Critical Anaysis Of Digital Signature Laws in India' (2018) 1 (4) IJLMH, <https://www.ijlmh.com/wp-content/uploads/2019/03/Critical-Analysis-of-Digital-Signature-Laws-in-India.pdf> accessed 12 June 2022

[5] Information Technology Act, 2000, s 2(1) (p)

[6] Information Technology Act, 2000, s 3

For the originator, it helps to encrypt an electronic transaction through a private key. Thus this creates a private wrap of that content and does not allow for modifying, altering, or even tampering with it after that the originator is assured that the information would not leak.

For the recipient, now the document can only be opened through the public key of the originator and then gets decrypted. If the e-record is able to decrypt with the help of the public key of the former then cannot be denied, but if the e-record is unable to verify its authenticity then it refers that there have been some alterations in the record which can be later detected.

For the legal system, the algorithm which is generated with the hash code helps create legality and accuracy of the record electronically. This system is called affixing digital data in short. Under the 2000 IT Act the entrusted authority called the Controller of Certifying Authority has the responsibility to maintain, the issue by taking necessary steps for safeguarding this process.

Suppose, Person A wants to send a message to Person B, and the former using his private key transfers a particular message through a hashing process or code such process is called encryption and with the use of the public key of Person A the decryption process starts wherein the hash value of the message will be compared with the final hash value and if both the values are similar then the transaction is valid and the signature is authenticated. This is known as the general concept of digital signature. This process of verification takes a matter of seconds and is one of the key players in e-commerce.

A certificate of digital signature ensures that no alterations are made to the data once the document has been digitally signed. The Act of 2000 provides for use of digital signatures submitted in electronic form in order to tonsure the security and authenticity of the document filed electronically. The concept of a digital signature is used in blockchain to sign transactions.

ROLE OF CERTIFYING AUTHORITY

Section 21(1)(g)[7] under the Act of 2000 states a person who grants a license for the issue of electronic certificates. The IT Act under its Section 21[8] also provides the process of obtaining a license wherein an application has to be submitted to the Controller with subject to the criteria included. Later on, after the submission Section 24[9] provides whether it must be granted or not. The next provision of Section 35[10] involves the process of making the application to the concerned authority where expenses shall not exceed Rs.25000/- provided that all the rules and regulations must be in accordance with the Act of 2000.[11]

LEGAL ASPECT

The Act of 2000 provides provisions under sections 66C, 71, 73, and 74[12] related to the punishment of identity theft with imprisonment of up to three years or a fine of one lakh or both, misrepresentation of a material fact, or suppression of such to the Controller of Authority with imprisonment of two years with fine or just a fine of one lakh, publication of false signature and creation or providing a certificate with fraudulent purpose which may lead to imprisonment of two years with fine or fine to one lakh.[13] In addition to this, in section 2(ta)[14] of the Act the term electronic signature is described as "confirmation of any electronic record by a supporter by methods for the electronic procedure determined in the subsequent timetable and incorporates advanced signature" and under Section 2(p)[15] characterised the

[7] Information Technology Act, 2000, s 21(1) (g)

[8] Information Technology Act, 2000, s 21

[9] Information Technology Act, 2000, s 24

[10] Information Technology Act, 2000, s 35

[11] Uday Bhatia, 'E-Signature: Bane OR Boon' (*Ipleaders,* 30 March 2020) <https://blog.ipleaders.in/e-signature-bane-or-boon/#Offences_relating_to_e-signature> accessed 12 June 2022

[12] Information Technology Act, 2000, ss 66C, 71, 73, and 74

[13] Yogesh Prasad Kolekar, 'Electronic Signature-Legal and Technical aspect' (*Legal Service India*) <http://www.legalservicesindia.com/article/1827/Electronic-Signature:-Legal-and-Technical-aspect.html#:~:text=The%20only%20method%20of%20authentication,of%20information%20technology%20Act%202000> accessed 12 June 2022

[14] Information Technology Act, 2000, s 2(ta)

[15] Information Technology Act, 2000, s 2(p)

term Advanced Signature.[16] Under the criminal law, where there is reason to believe that any person has dishonestly fraudulently signed, transmitted, or sealed ant legal record with an electronic signature leads to the punishment of two years with a fine or fine under SECTION 465[17] of the Code of 1860.

COURT CASES

Bergson v Gogo LLC[18]

The defendant, an inflight WiFi provider in airports and airlines to passengers, mislead its customers into purchasing a service package that would automatically renew the subscription without any prior notice. Here the plaintiff Adam Berkson and Kerry Welsh sued the company where they were charged $35 and $40 each for 3 and 16 months. The case was brought to US District Court and explained the concept of a click-wrap agreement which requires a click to accept the terms and conditions button before entering into a contract. The defendant claims that they provided such a facility on their website but it was observed that the terms and the conditions were not displayed in a proper font. It was merely projected through a hyperlink which is not a complete disclosure and thus the plaintiff cannot be bound by it. The court further adds purporting to represent a class, if the plaintiff alleges:

- That he himself has personally suffered some actual injury as a result of the illegal conduct of the defendant and
- That such putatively illegal conduct has raised the same set of concerns and has allegedly caused injury to the other members of the same class by the class of the defendants.

[16] Rohith R. & Ragavee U, 'A Critical Study on Digital Signature andits Security in India' (*ILSIJLM*, 17 January 2020) <https://ilsijlm.indianlegalsolution.com/a-critical-study-on-digital-signature-and-its-security-in-india-rohith-r-ragavee-u/> accessed 12 June 2022

[17] Indian Penal Code, 1860, s 465

[18] *Berkson v Gogo LLC* [2015] 97 F. Supp. 3d 359 (E.D.N.Y. 2015)

Zakuski v General American

This case marks one of the landmark cases in the field of Electronic signatures. The case concerns an insurance policy taken by the plaintiff in the name of his mother but as soon as remarried, the plaintiff changed the beneficiary's name to his second wife, to the other policies as soon after which the doctor Z, was expired. Later the plaintiff sued the company for a claim with the contention that the defendant cannot make sure it was the plaintiff's son who actually signed to verify it. The judgement follows in favour of the defendant because the insurance company had informed the plaintiff with an alert email confirming the change of beneficiary name.

Adams v Quicksilver (2010)[19]

The case records in California where an agreement had been sent to the offended party by means of a hyperlink in an email where the party had to sign one was towards the part of the arrangement. Later on, the question that arose was the legitimacy of the party's electronic mark on the business contract.[20]

E-Aadhaar Case

The issue relates to a password-protected copy of Aadhaar which is signed electronically by the competent authority of the Unique Identification Authority of India, UIDAI. The project was initiated in 2009 by the Central Government addressing the issue of leakages in various government welfare schemes and welfares like Voter ID, Ration Card, and Driving licenses which sapped bureaucratic corruption and red tape using two bases of information; Biometric information and Demographic information.[21] Parliament even enacted laws in 2016 Aadhaar Targeted Delivery of Financial and Other Subsidies Benefits and amendment of section 139AA under Services the Act and Finance Act of 2017. The court ruled in the majority of the provisions under the Acts as constitutional according to Article 21[22] of the Constitution.

[19] Adams v Superior Court (Quicksilver, Inc.) (2010) L. A. No. 24621

[20] Rohith R., & Ragavee. U (n 16)

[21]Uday Bhatia (n 11)

[22] Constitution of India, 1950, art.21

Provisions under Sections 7, 33 (amended), and 57 of the Act mentioned above were held to be valid on the basis of the test of proportionality.

CONCLUSION

E-Commerce has improved in nations worldwide. The fundamental concept of the Digital Signature has advanced the answer for validity in web-based transactions as a legitimate assurance to the data and protection against various issues. E-services today are increasing day by day with a positive success rate in mechanisms like shopping, governance, learning, etc. this completely depends on the validity, integrity, security, and authenticity of the subject matter that is being transmitted in a matter of seconds from the sender to receiver. Another type is a digital signature which performs a complex algorithm using its essentials to decode a message to check its legality. The initiation of multiple methods would help prevent crimes in the virtual world and ease the transactions happening online today and future.[23]

[23] Dr. Abhishek Roy & Sunil Karforma (n 1)